Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual Section 64.2009(e) CPNI Certification for 2011 covering the prior calendar year 2010

1. Date filed: March 1, 2011

2. Name of company covered by this certification: e-vergent.com, LLC

3. Form 499 Filer ID: [New]

4. Name of signatory: Michael Falaschi

5. Title of signatory: Managing Member

6. Certification:

I, Michael Falaschi, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed Michael Falaschi, Managing Member

Attachments: Accompanying Statement explaining CPNI procedures

CUSTOMER INFORMATION POLICY

To protect the proprietary and private information about our customers, e-Vergent.com, LLC, establishes this company policy regarding customer information:

1. All of the company's proprietary data bases, including that containing customer information, are password protected, and access to same is limited to authorized personnel only. Distribution of the password is limited to those authorized personnel. The password will be changed routinely, and whenever an employee with access to such data bases leaves the company.

2. No customer information in any form is to be removed from the company's offices by employees or others. This includes computer printouts, handwritten information or notes, copies of files or documents in any electronic form, and verbal transmission of customer information to persons who are not direct employees of the company.

3. Employees are to closely guard customer lists, contact information, telephone numbers, mobile code lists and all other customer information, both proprietary and public, to prevent any information from being removed from our offices by non-employees either accidentally or intentionally. Records are maintained for at least one year of the sales and marketing campaigns of the company or of any affiliate that uses customer CPNI. Sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

4. The notes that a salesperson may make about a customer must be returned to the company's office and re-filed or shredded. This information is to be shared only with the customer. At the completion of the sales call, the information is to be returned to the office and re-filed or shredded.

5. Internal documents, notes made when customers call in, and anything containing customer names and telephone numbers must be shredded at the end of the business day.

6. Each new customer is required to select a personal password and provide the company with certain non-public information that only the customer knows, such as a favorite pet's name, etc., which password and information is to be used for identification purposes. Upon contact with a customer, you must request that the customer confirm his/her identity by providing you with his/her pre-existing password and pre-selected information before discussing any matter with the customer. If a customer visits the company's retail local and requests access to CPNI, the customer must first present a valid photo ID matching the customer's account information. Customers are to be notified immediately when there are changes in a customer's password, online account, address of record or any authentication information.

7. Customer information is never to be used or disclosed to anyone, except as follows:
   (a) to market the company's service offerings to which the customer already subscribes;
   (b) to market the company's CPE, information services, and adjunct-to-basic services;
   (c) for purposes of conducting health effects research;
   (d) to protect the company's own rights and property, and to protect the rights of other carriers or other users of services from fraudulent, abusive or unlawful use;
   (e) to disclose all location information in emergency situations, as provided for under §§222(d)(4) & (f) of the Communications Act of 1934, as amended;
   (f) to comply with the company's obligations to provide certain customer information when lawfully requested by law enforcement authorities pursuant to the Communications Assistance for Law Enforcement Act ("CALEA"); and
   (g) to resolve specific customer questions about the customer's own account, arising in the course of a telephone conversation between that customer and company's service representative, and then only after orally obtaining from the customer a limited, one-time authorization to use the customer's information for the duration of that phone call.

8. Disconnected or inactive customer files are to be retained for no more than 3 years, and then shredded. Disconnected or inactive customer files are never to be placed in the trash unshredded. Customer database printouts are to be shredded when replaced by newer printouts.

9. Our company has a notification process in place to alert law enforcement, the FCC and affected customers in the event of a CPNI breach.

10. Appropriate disciplinary action will be taken for any violations of this policy.